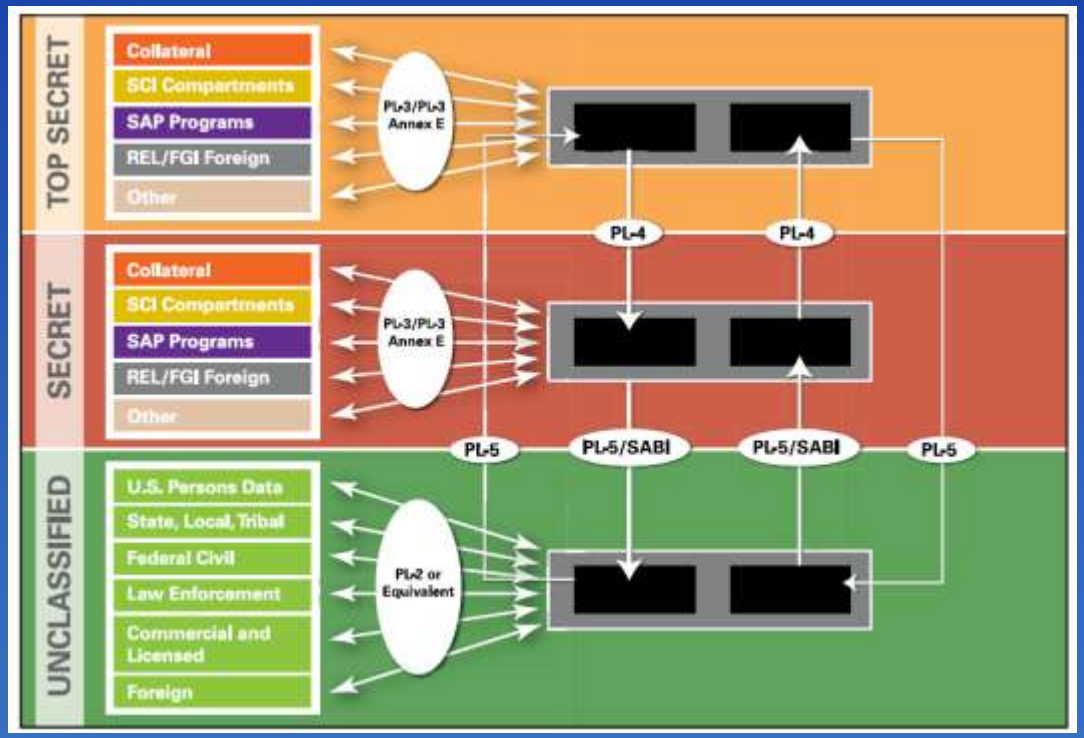


eXMeritus

HardwareWall™

Secure Data Transfer System

Presented by
Thomas Rooney
The Boeing Company

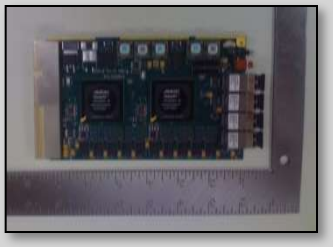
Overview

- **Company Profile**
- **HardwareWall™ Overview**
- **v2.9.2 Specifics**
- **Baseline Solution**
- **Configuration and Applications**
- **Objectives for Baseline Updates**
- **Product Development Roadmap**

Company Profile

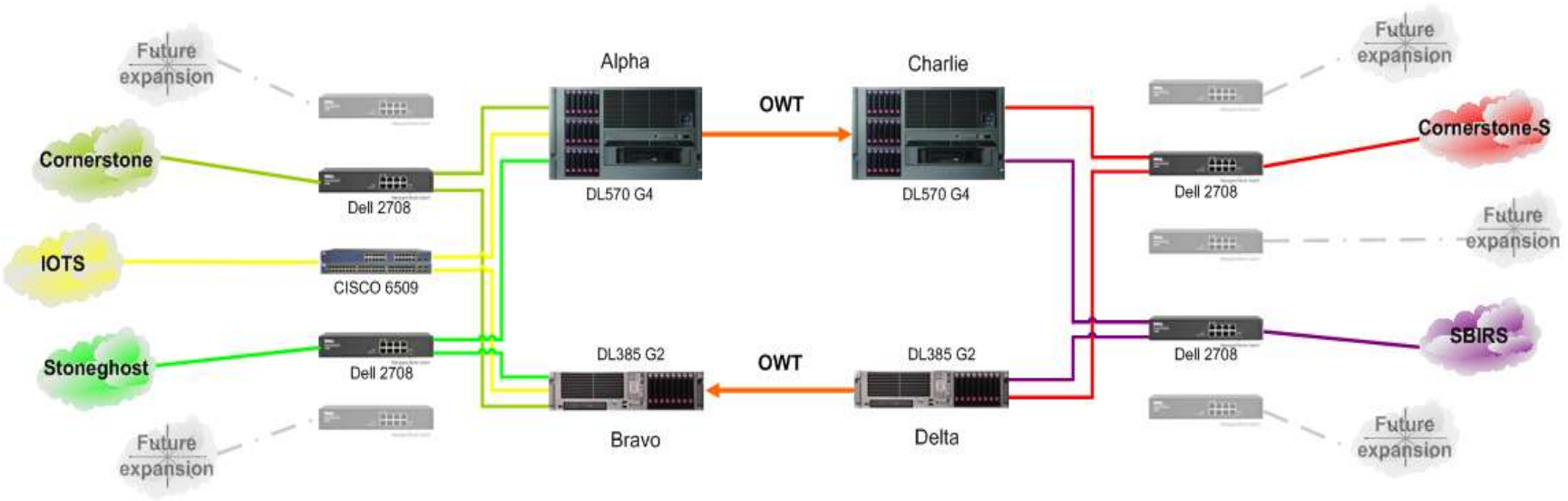
Network & Space Systems | Space & Intelligence Systems | Mission Systems

- Developer of highly-capable, cost-effective, cross domain solutions
- Started as a private company in 2000 in Fairfax, VA
  - Founders: Thomas Rooney & Robin Alman
- Employees: was 15 full-time plus part-time interns prior to acquisition
- Acquired by The Boeing Company on June 19, 2009
- Highlights:
  - First bi-directional PL-4 delivered in 2000 and accredited January 2001
  - First bi-directional PL-5 delivered in 2003
  - First flight qualified and TEMPEST hardware delivered in 2008; accredited in 2008
- Customers: Intelligence Community, Department of Defense and their contractors



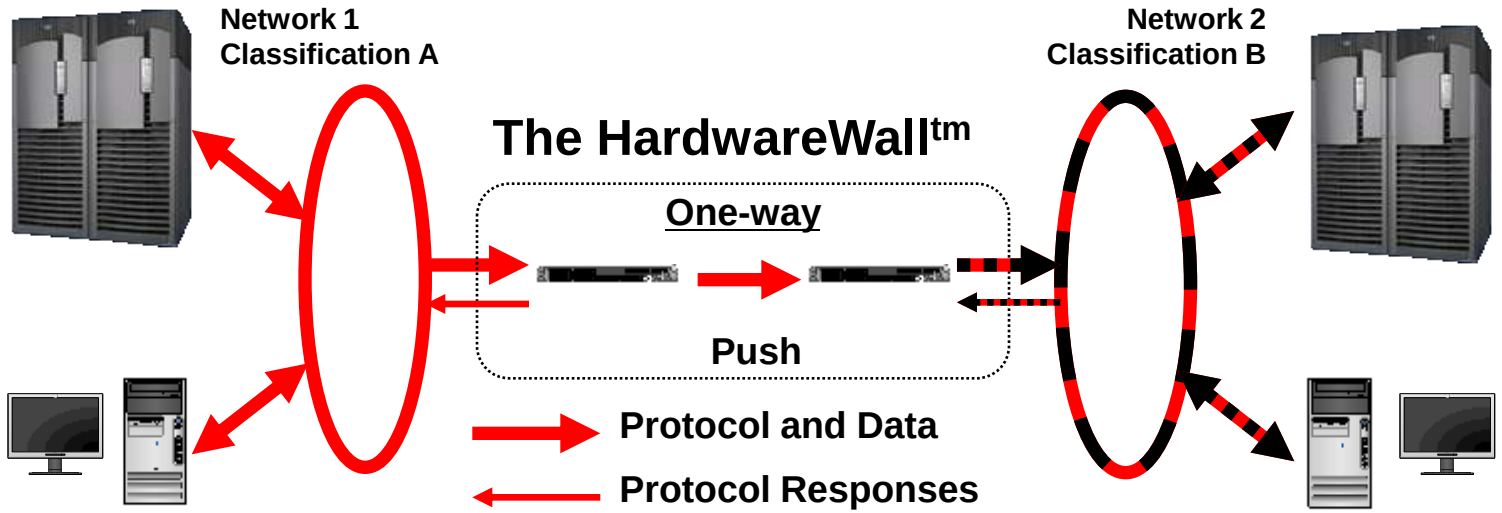
What is HardwareWall™?

- **Transfer solution**
- **Used for high-to-low, low-to-high, bidirectional, data transfer**



What is HardwareWall™?

- **Software solution**
- **Incorporates physical one-way transfer**
- **Assembles in segments to support complex interconnections**



What is HardwareWall™?

- **Full-featured guard solution**
- **Tightly coupled with a “trusted” operating system**
- **Proxies services for transport**
- **Performs content review prior to release**
- **Provides access control and restricts transfer based on source, destination, service, and data type**

What is HardwareWall™?

- **Operating systems supported**
  - **SELinux® - primary, Baseline solution, recommended for all new installations**
  - **Solaris® 10 with Trusted Extensions – legacy, not recommended for new installations**
  - **Trusted Solaris™ - no new installations**
  - **IRIX® - no new installations**
- **Processing architectures supported**
  - **x86 – primary for high data rate and fixed-facility implementations**
  - **PowerPC – primary for small form factor implementations**
  - **SPARC – no new installations**
  - **MIPS – no new installations**

HardwareWall™ v2.9.2

- **Version Numbering**
  - **Version number typically increments concurrent with an accreditation**
  - **v2.9.2 is March 2008 version of HardwareWall™**
  - **Similar software architecture to original version 2 (Trusted Solaris™, 2003)**
  - **First system delivered in SELinux®**
  - **Similar in architecture and implementation to current deliveries**
  - **Current version is 2.12**

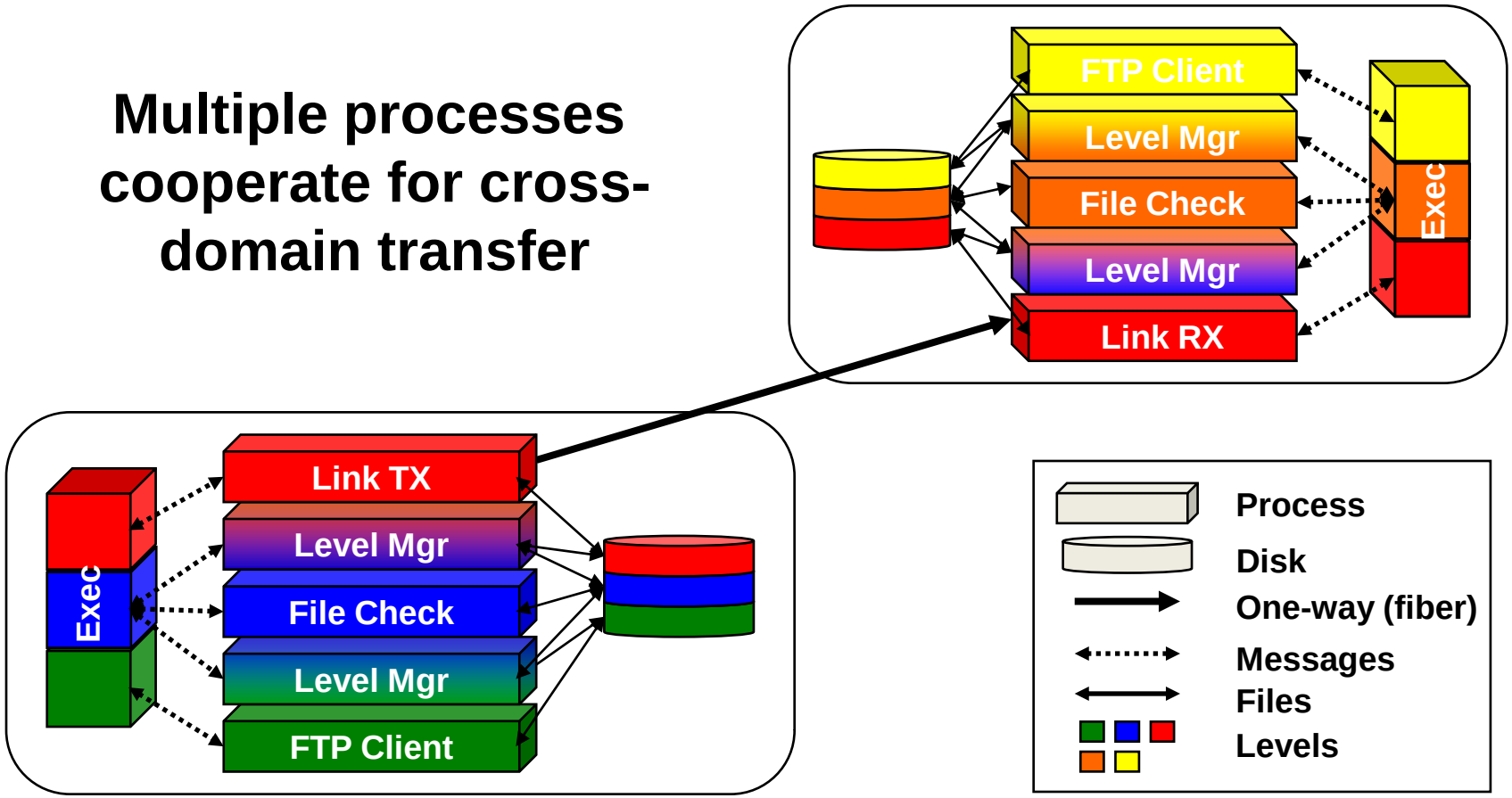
HardwareWall™ v2.9.2

- **Construction**
  - **Multiple processes within “trusted” operating system**
  - **Separate processes for:**
    - **Data transport**
    - **Internal movement between MAC labels**
    - **Content review**
    - **One-way transfer**
  - **Cooperation of all processes required for transfer**

HardwareWall™ v2.9.2

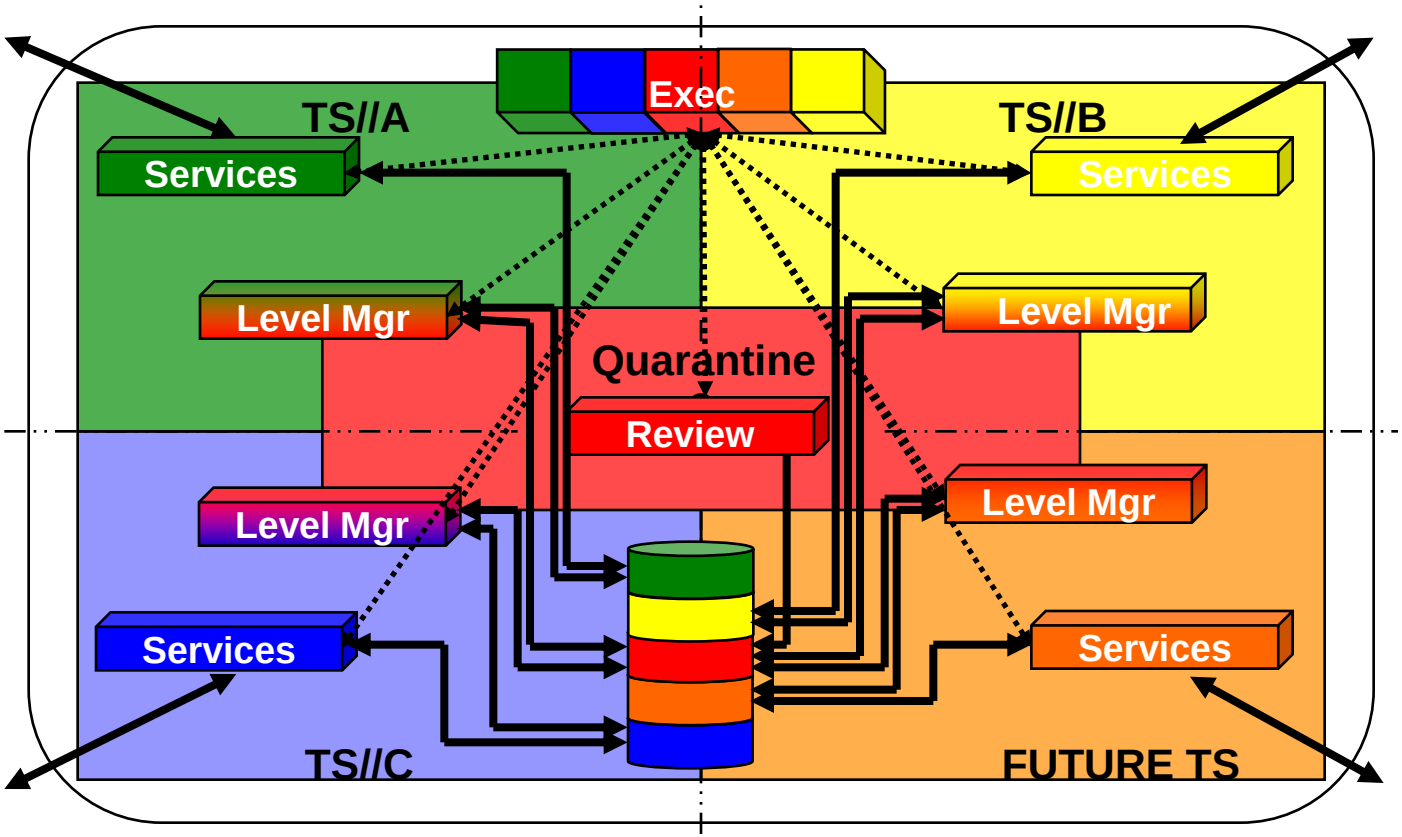
Construction Example – Low-to-High Transfer

Multiple processes cooperate for cross-domain transfer



HardwareWall™ v2.9.2

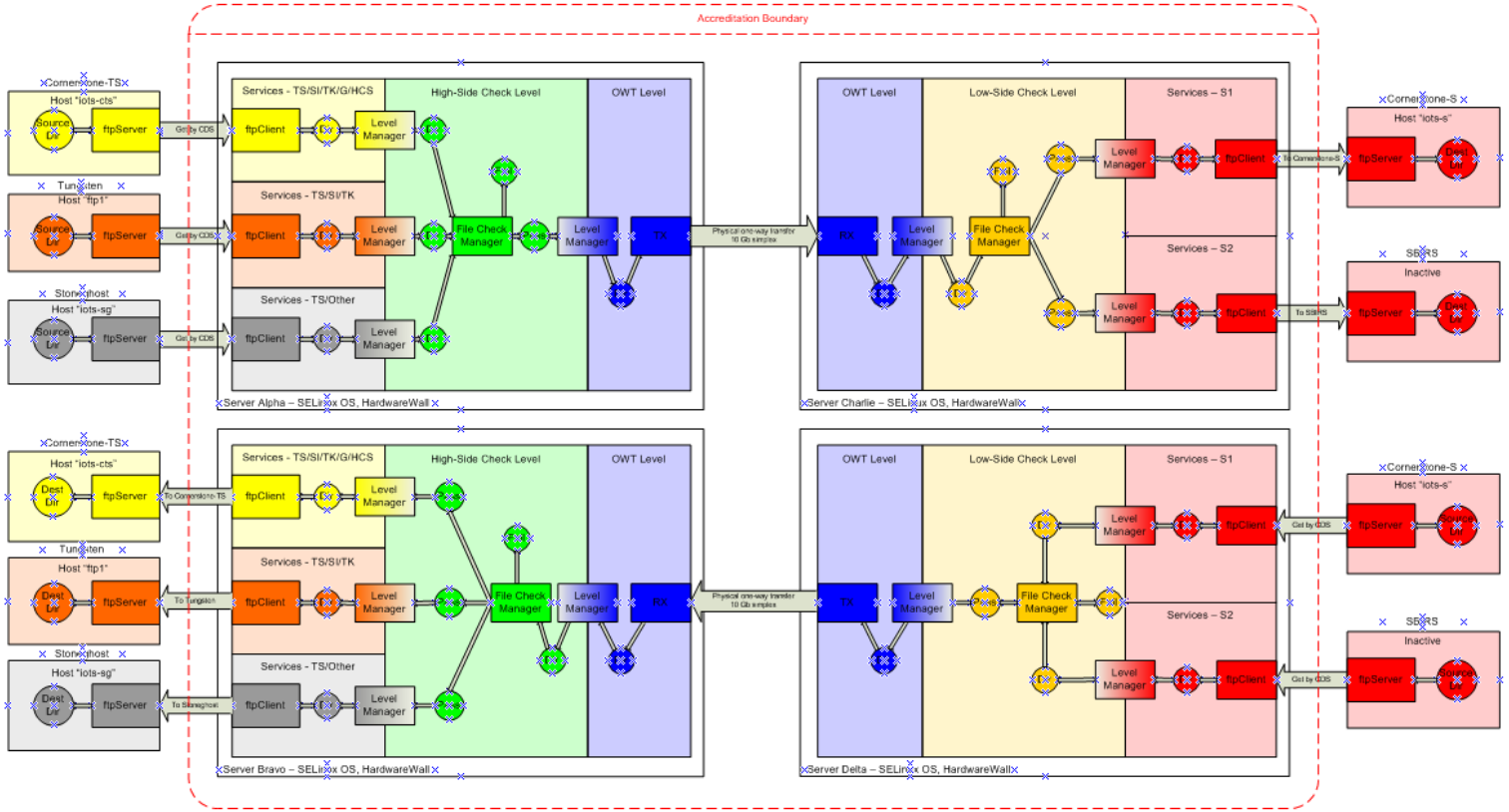
Construction Example – PL-3 Transfer



Multiple processes cooperate for cross-domain transfer

HardwareWall™ v2.9.2

Construction Example – Baseline System



Example configuration for interconnection of five domains

HardwareWall™ v2.9.2

- **Processes Available in v2.9.2**
  - **LinkExec - Controls routing among processes, starts and monitors all processes**
  - **FtpClient (depreciated) – file transfer via File Transfer Protocol (FTP)**
  - **TransferClient – file transfer via multiple protocols**
  - **Directory Manager – directory scanning**
  - **CommandServer – streaming data connectivity and content review**
  - **Filter – XML content review and redaction**
  - **New File Relay – remote tasking and status**
  - **Level Manager – movement of data between MAC levels**
  - **FileCheckManager – content review for files**
  - **LinkTransmitter – one-way transfer**
  - **LinkReceiver – one-way transfer**
  - **FileRename – utility process to relocate and rename files**

HardwareWall™ v2.9.2

- **Key Feature – Defined interfaces among processes**
  - **Pipes for communication with executive process**
  - **Command, response and error messages**
  - **UNIX domain sockets for streaming data**
  - **Shared memory no longer recommended**
  - **TCP / SSL / TLS sockets to support remote tasking and status**

HardwareWall™ v2.9.2

- **Key Elements of HardwareWall™ Architecture**
  - **Multiple processes cooperate for cross-domain transfer**
  - **One-way transfer adds to protection against attack**
  - **Modular design**
    - **Easy to add new sources, destinations, levels and data types**
  - **Processes made interchangeable by standard interface among processes**
    - **Easy to add new processes and protocols**

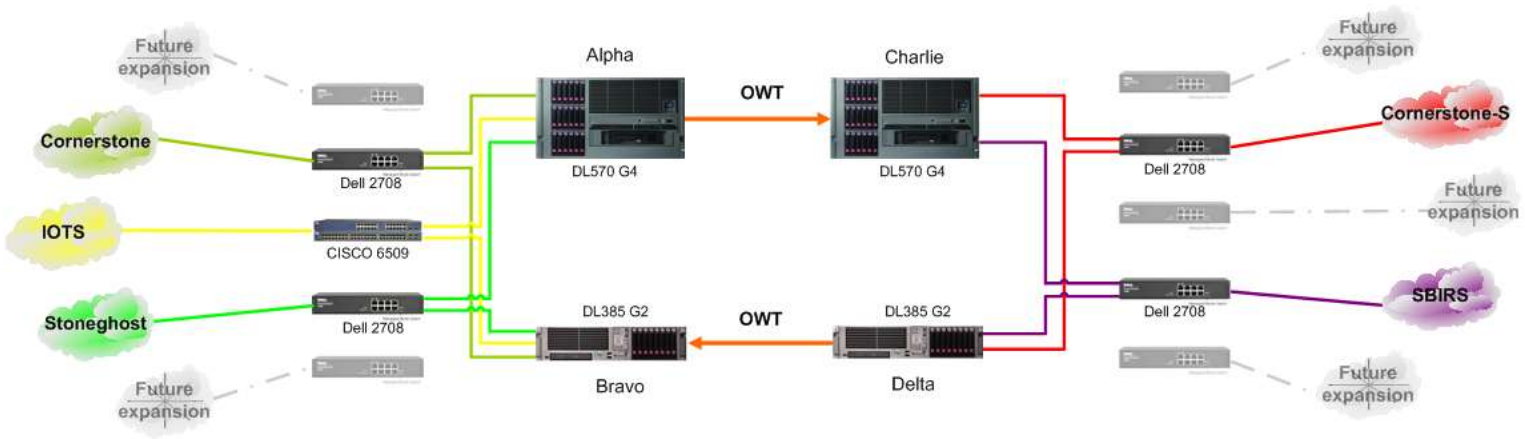
HardwareWall™ Baseline Solution

- **Why is HardwareWall™ on Baseline? (our perspective)**
  - **Similar in many ways to other cross domain solutions**
    - **Implements MAC, DAC, content review, auditing, etc.**
    - **Establishes a barrier between disparate domains**
    - **Performs content review prior to release**
  - **Slightly different combination of capabilities**
    - **Incorporates one-way transfer and traditional 'guard' capabilities**
    - **Uses many processes, each performing a small role and tightly bound in level and privilege**
  - **Capable of high-speed, large file transfer**
    - **Solution needed for transfer of imagery and other GEOINT data types**
    - **Submitted as filling gap for sustained high-speed transfer of GEOINT (formerly MASINT) products**

HardwareWall™ Baseline Solution

Nested PL-3 / PL-4 / Annex E for transfer of GEOINT among multiple networks

- **Transfers MASINT and supporting data among multiple networks**
- **Key features include**
  - **Large binary file dissemination**
  - **Diverse product dissemination**
  - **Large binary file ingest**
  - **Diverse supporting file ingest**
  - **Pre-configured for incorporation of additional networks**

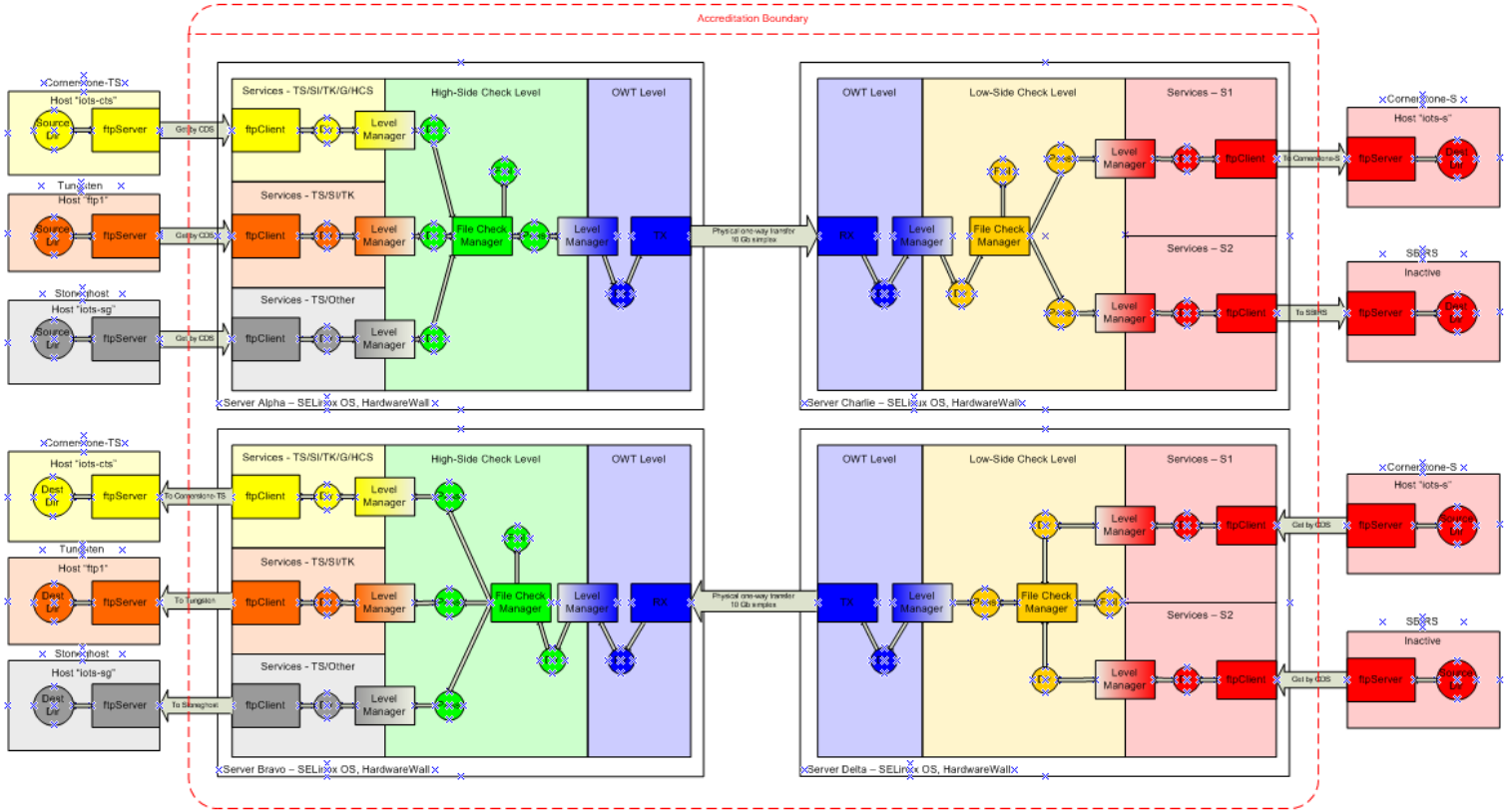


HardwareWall™ Baseline Solution

- **Technical Details**
  - **Implemented in SELinux® (Red Hat Enterprise Linux v5)**
  - **Implemented on x86 servers (HP DL385 and ML570 servers)**
  - **Runs in Enforcing mode using both strong typing and data labeling**
  - **FTP (depreciated) used for file transfer (required to not impact supporting systems)**
  - **Content review methods include**
    - **Field-by-field format and content review**
    - **Signature review**
    - **Review of internal classification tags**
    - **Virus scanning**
    - **Regular expression (“dirty word”) available but not used**

HardwareWall™ Baseline Solution

Baseline System Routing



Simple interconnection of five domains

HardwareWall™ Baseline Solution

- **Example data types**
  - **Spectral Frame Products**
    - **Structured multispectral data format**
    - **Fields containing metadata and large binary segments containing calibration and collected data**
    - **Field-by-field review conducted to ensure compliance with data specification**
    - **Internal classification labels reviewed against level(s) of intended destination(s)**
    - **Digital signature reviewed to ensure file was not modified and to confirm authorization for release**

HardwareWall™ Baseline Solution

- **Example data types**
  - **Analyst signed intelligence products**
    - **Highly-diverse set of products**
    - **Signed by analysts authorizing release**
    - **Digitial signatures verified to confirm integrity and authorization for release**
    - **Analyst-applied classification tags reviewed against level(s) of intended destination(s)**

HardwareWall™ Baseline Solution

- **Example data types**
  - **Large binary data products (ingest)**
    - **Highly structured files with very large binary segments**
    - **Reviewed for compliance with data specifications**
    - **Compliance with format and content ensures file is not malicious code**
  - **Supporting data (ingest)**
    - **Highly diverse set of files**
    - **Scanned using conventional virus scanner**

Configuration and Applications

- **Configuration files define:**
  - **Sources**
  - **Destinations**
  - **Processes to be started**
  - **Operation of each process**
  - **Routing among processes**
  - **Content review methods**

Configuration and Applications

- **Configuration File Examples**
  - **Commands to start a participating process**

```
###############################################################################
###
###  UNCLASSIFIED UNCLASSIFIED UNCLASSIFIED UNCLASSIFIED
###
###  Copyright (C) 2001-2008 eXMeritus Software Federal Systems, Inc.
###  All rights reserved.
###  This notice does not imply publication.
###
###  Description:
###   /HardwareWall/Configuration/alpha/alpha_TransferClientA.command
###   TransferClient command file for high-side transmit machine,
###   hostname designation ALPHA.
###   Please see http://www.exmeritus.com/support.html for more
###   information.
###############################################################################

1  COMMAND        /HardwareWall/bin/TransferClient
2  PROCNAME       TransferClientA
3
4  ARGUMENT       -
   c/HardwareWall/Configuration/alpha/alpha_TransferClientA.config
5  ARGUMENT       -l/data/logfiles/alpha/TransferClientA/
6  USEDIR         /data/logfiles/alpha/TransferClientA/          770
7  USEDIR         /data/working/alpha/TransferClientA/           770

8  USER          highservA
```

Configuration and Applications

- **Configuration File Examples**
  - **File transfer using SFTP pull**

```
2   NUMTHREADS 1
3   WORKDIR /HardwareWall/working/TransferClient/
4
5   # This is a polling task polls a directory on the local machine every 30
    seconds, forever.
6   TASK Poll
7     ACTION LIST
8     FILETYPE 100
9     ROUTENUM 10
10    FILEPERM 520
11    NUMREPEAT -1
12    REPEATSEC 30
13    URI SRC
14      PROTOCOL FTP
15      USER root
16      PASSWD rootme
17      HOST 192.168.0.250
18      #PORT 21
19      PATH /data/working/source/
20      FILENAME *.tar
      END-URI
21    URI DST
22      PROTOCOL FILE
23      PATH /working/username/tmp/
24      HOST localhost
25    END-URI
26  END-TASK
```

Configuration and Applications

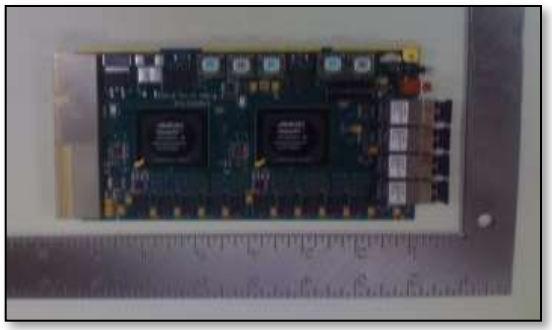
- **Configuration File Examples**
  - **Extracts from a complex rule set**

```
# NITF - NITF Ruleset Configuration File
#       NITF
#
# Developed by eXMeritus Software, Inc.
#


# record once containing entire config
# 1
record name TopRecord once elements 0
  # 1-1
  value fileStart getoffset
  end-value

  # 1-2  # check version of NITF
  value VERSION string
    constraint allowed 2 NITF02.00 NITF02.10
    format
      width 9
      maxwidth 9
      maxleadws 0
      rigid true
    end-format
  end-value

  # 1-3
  # opens NITF versions
  record name VersionCheck permitted using VERSION value keys 2
    NITF02.00 => elements 1
      record name NITF2_0 seekoffset using fileStart beg
      open /HardwareWall/Configuration/FCM/NITF2.0/Master/NITF_A1_FileHeader.config elements 1
      end-record
    end-record

    NITF02.10 => elements 1
      record name NITF2_1 seekoffset using fileStart beg
      open /HardwareWall/Configuration/FCM/NITF2.1/noticeTWO/NITF2.1_A1_FileHeader.config elements 1
      end-record
    end-record

  # end 1-2 record permitted
  end-record

  value DIGISIG signature
    format
      quoted true
     form-string "%Y/%m/%d %H:%M:%2SZ"
    end-format
    keyDir /HardwareWall/Configuration/keys/
  end-value

  record name VALIDATE_SIG signed

    signature using DIGISIG
    offset using fileStart beg
  end-record

end-record
```

Configuration and Applications

- **Availability for Linux® supports many platforms**
  - **Enterprise-class solutions**
  - **Ruggedized solutions**
  - **Embedded solutions**

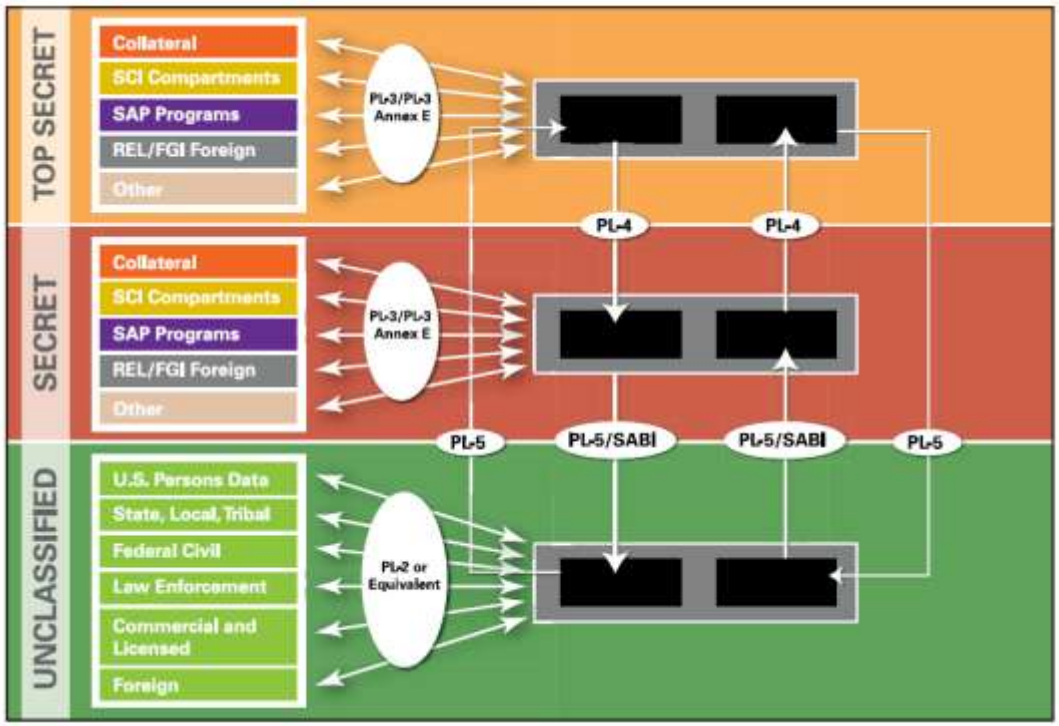
2U flight-qualified appliance



Compact PCI card

Configuration and Applications

- **Modular construction supports interconnection of many domains**



Objectives for Baseline Updates

- **Many protocols supported in v2.9.2 but not used in application submitted Baseline review**
- **Many protocols and services implemented in other accredited solutions but not submitted for Baseline review**
- **Current version is 2.12**
- **Our objective is to submit evidence for current version and other accredited protocols for Baseline review**

Objectives for Baseline Updates

- **Many protocols supported in v2.9.2 but not used in application submitted Baseline review**
- **Many protocols and services implemented in other accredited solutions but not submitted for Baseline review**
- **Current version is 2.12**
- **Our objective is to submit evidence for current version and other accredited protocols for Baseline review**

Product Roadmap

- **Add current capabilities and version to Baseline list**
- **Develop whitepapers for application of current capabilities (e.g. data flow for use of "sidecars")**
- **Automated configuration using DFCF / BRAY**
- **Extend current XML support**
  - **Additional libraies for diverse schema review**
  - **Add capabilities for transformation (XLST) and Schematron**

Product Roadmap

- **Extend support to small form factor and rugged applications**
- **Expand prototype capabilities for cross-domain search and cross-domain work flow to enterprise-class, Baseline capabilities**
- **Expand prototype capabilities for cross-domain identity management to an enterprise-class, Baseline capability**
- **Add robust support for cross-domain mail**

Contacts for Additional Information

- **Basic information – www.exmeritus.com**
- **Sales – sales@exmeritus.com**
- **Support – support@exmeritus.com**
- **Direct – 703-764-0925**
- **Web site and all e-mail addresses will migrate to Boeing**